

**This is a clean copy containing 38 pages**

## Disposable Financial Tools

### CROSS-REFERENCE TO RELATED APPLICATIONS

#### U.S. PATENT DOCUMENTS

U.S. PATENT. NO. 4,594,663 JUNE 10, 1986. NAGATA, et al.

### STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

This invention is not associated with any federally sponsored research or development.

### BACK GROUND OF THE INVENTION:

#### FIELD OF THE INVENTION

Present invention relates to disposable financial tools (DFT), particularly those tools that are used to access cash and credit account. More particularly, the invention relates to a method and system for carrying out cash and credit transaction, without revealing the account number to the merchant or payee during a purchase or charge back transaction. Specifically to improved security for the account while carrying out transaction in person and on the Internet, creating an improved fraudulent prevention system, with out publish the account number on checks and credit cards that can be viewed.

#### DESCRIPTION OF THE RELATED ART

Present financial tools like credit card can be used multiple times, and the account number is expose to every merchant where the card has been used to carry out transaction. A single check can be re-deposited multiple times until it is cleared. Such financial tools do not ensure safety to the account, because they reveal the account number, expiration date, name and address of the account holder to the merchants and employees, who could reused the publish account number on the checks and credit cards. A credit card user having a subscribing account with a merchant, who wants to unsubscribe from the account and someone who is using an automatic or recurring billing method with an e.merchant, runs into problems when his credit card account is change. The merchant sometimes present the old account number and expiration date multiple times to the credit card company who then turnaround and bill the user new account number, even if the user hasn't received the new card with the new account and without the new card been activated unknowing to the account holder. They only ensure access to the account so long as the routing number (ABA) number, account number, branch number, expiration date, check number is correct, and enough cash or credit in the account to cover the transaction with a signature, fake or real. For example, no signature is required on a check or credit card transaction when making an Internet purchase or for off-line transaction, but the transaction will be approved. Even in person a credit card or check can be used with a fake signature. In such cases, the user only needs to get an approval after processing, while the merchant only look forward to an approval and sometimes match the signature. With fraudulent check and credit card

transaction, most of the time the account holder only finds out that his cash or credit has been depleted after getting his statement or get a notice of a bounce check. In many cases, the only thing that is needed is enough cash or credit for the check to be cleared or credit transaction to be approved. The safety of present financial tools like checks and credit cards are left for the account holder and payee or merchant to determine if the check/credit card is own by the payer. The account number of a check is published on the check, and a credit card carry's the account number publish on the card with the expiration date. Sometimes invoice or receipt carries the credit card number with the expiration date when a purchase is made, making them vulnerable for fraud and counterfeit. Merchants have the power to enter any amount when making offline transaction. E.commerce has made credit card and checks very vulnerable, increasing identity theft since becoming mainstream.

There is a need to create a more secure method and system to prevent credit card and check fraud that leads to identity theft. Using an effective system and method would prevent merchants and or payee from seeing or having access to the payer account number on a check and credit card and the expiration date on the card, when making a purchase or during a charge back transaction.

#### BRIEF SUMMARY OF THE INVENTION:

It is an object of the invention to provide a method and system for implementing Disposable Financial Tools (DFT), with cash and credit accounts that would eliminate fraud associated with identifying the prior art and enhanced performance of fraud protection. The invention also comprised of a method with unique working life exit (drone) numbers and access to a fix/limited and or unlimited amount of cash or credit in an account. When used to make a purchase, it cannot be reused or redeposit unless the working life is extended by the issuer or processing network (DFT), because the Drone/exit number drop off and die by been place in an inactive mode. Another method of the invention includes providing at less two sets of numbers, a central number (queen number) and a secondary number (Drone/exit number) when using multiple account issuers. The drone and queen number together forms a bundled number. Drone and bundled numbers are place on check style formatted card, and work together with an ID number for identifying a portable remote electronic financial apparatus with or housing Drone/exit, check and or bundled numbers. The portable remote electronic apparatus also house an electronic book (electronic check book apparatus/remote electronic check book) with electronic check and a electronic web card. When the queen (Q) number and Drone (D) numbers (bundled number) integrate or come together to carry out a transaction on the IEI (DFT) network, by been exactly in accordance or matching the sets of numbers (bundled number) or the drone number with those on the private (DFT) network or instant enhance Internet network (IEI network), if approved when process on the private (IEI/DFT network) the customer checking or credit card account number provided for billing and transaction amount or drone number, transaction amount and account number would merge into the banking system, then move on to the merchant guarantee processor for a second approval or processing. The used drone (exit number) is automatically altered and lock on the private (DFT) network in an inactive mode blocking it from reentering the IEI/DFT network

and or banking system network after gaining access, process and approved on the private/iei network, in order to prevent a DFT with the same exit (Drone number) from gaining access to the banking system network again. The exit (Drone) numbers are altered or drop off and or die (in active mode) as a built in safety, whenever the exit (drone) numbers are in accordance/same with or marching the routing (ABA) number, account number, or PYN (payment number) and other secondary numbers (ATV, Sleet number) that are on the Iei network and or in the banking system. DFT does not carry an account number unlike checks and credit card. It carry's a central number (Queen/Q number), because the DFT Drone/Exit number is specific in its transaction, the working life has the capability of architecture for specific usage when making a purchase and or used in the form of a ticket/pass. Financial tools that reduced fraud and financial terrorism or identity theft. Financial tools for making purchases without an account holder worrying about someone stealing his accounts number or assuming his identity. Disposable financial tools method and system is effected by customer and merchant establishing an account with the issuer of disposable financial tools. Transaction is carried out manually by entering user name, address and drone or bundled number from a check style formatted card or a remote electronic financial apparatus. Automatic transaction is carried out by scanned or swipe user card and using a remote electronic financial apparatus/ portable remote electronic financial apparatus. The apparatus is turned on and point towards a payment gateway at check out, capturing the RFID/infrared signal from the payment gateway reads automatically displaying a light or word ready/set. User/customer would press pay/send button, to submit the encrypted drone or bundled number and apparatus ID number onto the payment gateway reader. Who then send it onto the private/ DFT network database for approval, if approved, the private/ DFT network send the user drone or bundled number with his checking or credit card account and the transaction amount or other financial account number to the merchant bank (banking system), without revealing the account number to the merchant or payee during a purchase or charge back transaction. DFT is charge back by entering the drone or bundled number with the option of the approved number. The check style formatted card or financial card and the remote electronic financial apparatus has the capability of carrying the Caribbean countries flag(s) and or Caricom countries flag(s) in paper, plastic and or electronic form. The DFT card(s) is/are not limited to a single drone or bundled number on the/a card(s). DFT system comprised of a computer network having payment gateway entry points, that allows a user to access the system with Drone (exit number), and or bundled number that is in active mode on the system, without logging to the user account; database for depositing and or holding user drone and bundled numbers, establish financial number, encrypted software, system operating software and software associated with a user portable remote electronic financial apparatus.

The foregoing and other objects, features, and advantages of the invention are now apparent from the following, particularly those descriptions of preferred diagrams of the invention as illustrated in those accompanying drawings.

# **BRIEF DESCRIPTION OF THE DRAWING:**

Figure: 101 show a front view of a sleek check with the holder and Issuer name. ATV #, space for placing Ads, and Sleek check stub.

Figure 102: shows a back view of a sleek check with space for Ads, payee name, memo, and authorized signature, Issuer name and address, Sleek check web address, expiration date and a magnetic strip covering the routing (ABA) number, branch number, with PYN/USFIN optional, ATV, and Sleek/check number.

Figure: 103 is showing a Sleek check receipt after a transaction is completed and approved.

Figure: 104 is a front view of a Sleek card, where third party logo and other drawing will be place.

Figure: 105 is a view of an illustrated primary holder Sleek card (Sleek P) appearance with a card number that has nothing to do with the transaction. But for end user use only (optional).

Figure: 106 is an illustrated front view of a Sleek –G for placing Companies Ads and other drawings.

Figure: 107 is an illustrated diagram showing a front view of a Sleek –G (sleek card gift card), with a space for reception/accountholder to write reception name as the payer and sign as the authorized signature on the card.

Figure: 108 An illustrated diagram showing a Sleek card receipt after a transaction is process and approved.

Figure: 109 is a diagram showing an IEIcard with its Queen and Drone number.

Figure: 110 is an illustrated diagram showing how the IEIcard loses its Drone (exit) number. Figure: 111 is a diagram showing a web template/payment gateway with a \$50 purchase.

Figure: 112 is an illustrated diagram showing an IEIcard web template/payment gateway for prospective buyers.

Figure: 113 Shows a web template after submit or pay is click on a payment page (gateway).

Figure: 114 Illustrates a payment and none payment gateway with a bundled number.

Figure: 115 Shows an illustrated diagram of a double processing system for drone and bundled number.

Figure: 116 Shows a simple remote financial apparatus.

Figure: 117 Shows an Iei multipurpose portable remote electronic financial apparatus.

Figure: 118 Figure: Shows an apparatus payment gateway for drone numbers.

Figure: 119 Shows a diagram illustrating an Iei payment gateway using bundled numbers.